

FILEDUNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO

UNITED STATES DISTRICT COURT

AUG 24 2016

for the
District of New MexicoIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Storage devices more fully described in Attachment A of
the AffidavitMATTHEW J. DYKMAN
CLERK

Case No. 16mr603

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A to the Affidavit

located in the _____ District of _____ New Mexico _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B to the Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

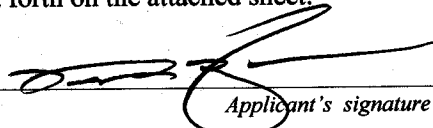
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sec. 2251(a)	Production of child pornography,
18 U.S.C. Sec. 2252(a)(4)(B)	Possession of child pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Ross Zuercher, Special Agent - FBI

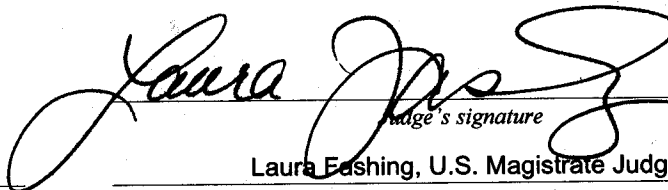
Printed name and title

Sworn to before me and signed in my presence.

Date:

8/24/2016

City and state: Albuquerque, New Mexico



Judge's signature

Laura Eashing, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

Your Affiant, Ross Zuercher, having been duly sworn, does hereby depose and say:

Introduction

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I have been a Special Agent (SA) of the Federal Bureau of Investigation (FBI), United States Department of Justice, since August 2012. As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search warrants. I am currently assigned to the FBI’s Albuquerque Violent Crime Program, as such, I am authorized to investigate crimes against children. The information set forth in this affidavit was derived from my own investigation and/or communicated to me by other sworn law enforcement officers of the FBI, Spokane Police Department and the Valencia County Sheriff’s Office. Because this affidavit is submitted for the limited purpose of securing a search warrant, your Affiant has not included each and every fact known to me concerning this investigation. Your Affiant has set forth only those facts that your Affiant believes are necessary to establish probable cause to support a search warrant for the items more fully described in Attachment B.

Relevant Statutes

3. This investigation concerns alleged violations of certain activities relating to material involving the sexual exploitation of minors; Title 18 U.S.C. §§ 2251(a) and 18 U.S.C. 2252(a)(4)(B)
 - a. 18 U.S.C. § 2251(a) makes it a federal crime for “[a]ny person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was

produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.”

- b. 18 U.S.C. § 2252(a)(4)(B) makes it a federal crime for any person who, “knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if—
 - i. the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
 - ii. such visual depiction is of such conduct.

Computers and Child Pornography

- 4. Computers and computer technology have revolutionized the way in which individuals interested in visual depictions of minors engaged in sexually explicit conduct (“child pornography”), as defined in 18 U.S.C. § 2256, interact with each other. Trading child pornography on the Internet is open, anonymous, and engaged in worldwide.
- 5. Your Affiant knows that computer hardware consists of all equipment that can collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, optical or similar computer impulses or data. Hardware includes any data processing devices such as central processing units, memory typewriters and self-contained “laptop” or “notebook” computers, iPads, iPods, Tablets, and Portable gaming devices, as well as internal storage devices such as fixed hard disks, floppy disk drives and diskettes, magnetic tape drives and tapes, optical storage devices, and other memory storage devices, as further described in Attachment B, incorporated herein by reference. Some computer hardware can be internal to the computer system or external. The external component hardware is often referred to as peripheral and includes input/output devices such as keyboards, printers, scanners, plotters, video display monitors and optical readers, web cameras, communication devices such as modems, recording equipment, RAM or ROM units, automatic dialers, video/digital camera equipment, flash drives, thumb drives, key drives, USB devices, removable/portable hard drives, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidisks, other optical disks, and other external media.

6. Your Affiant knows that computer files or remnants of such files on computers and computer related media can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a computer and/or computer related media, the data contained in the file does not actually disappear; rather, that data remains on the media until it is overwritten by new data. The actual file is not initially erased or removed from the computer and/or computer related media, but rather, it remains available in free space on the computer and/or computer related media until overwritten by other information. The "deleted" file can also be overwritten by information when the computer user takes a positive action to permanently remove the "deleted" file from the hard drive, such as employing "wiping" software, formatting the hard drive, or de-fragmenting or compressing the information located on the hard drive. However, "deleted" files which have not yet been overwritten by other information can often be successfully recovered during the search of a computer system or computer related media. These "deleted" files are often recovered long after the date the criminal activity occurred. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.
7. Your Affiant knows that computers and computer related media's ability to store images in digital form makes them an ideal repository for child pornography. A single DVD, CD-ROM, jump drive, hard drive, thumb drive, compact flash, other memory cards and other devices (as referenced in Attachment B) can store thousands of images and hundreds of thousands of pages of text, with storage capacities increasing all of the time. The size of the fixed electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the past several years. Hard drives with a capacity of one hundred gigabytes or more are not uncommon. These drives can store hundreds of thousands of images at a very high resolution. Electronic storage located in host computers adds another remote dimension to this storage equation.
8. Your Affiant knows through training and experience that people who possess or produce child pornography often keep child pornography on portable media devices. The use of portable devices for child pornography makes it easier for users to conceal and access remotely.
9. Your Affiant knows through training and experience that people who possess or produce child pornography usually place child pornography they collect on multiple devices as a backup.

10. Your Affiant knows through training and experience that people who possess or produce child pornography do not often dispose of the child pornography that is collected.
11. Your Affiant knows that computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical or other digital form. It commonly includes programs to run operating systems, applications such as word processing, graphics or spreadsheet programs, utilities, compilers, interpreters and communications programs.
12. Your Affiant knows that documents can be created through the use of computer software programs, and that those documents can be used to facilitate the commission of crimes. In some cases, the mere possession of certain types of documents constitutes criminal conduct. Computer systems also can store information in internal or peripheral storage devices including fixed disks, floppy diskettes, tape drives, optical storage devices or other memory storage devices such as flash drives, thumb drives, key drives, USB devices, iPods, iPads, PSP Players, removable/portable hard drives, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media. Based on my training and experience, and my personal use of computer systems in my employment as a Special Agent, I know that users of computer systems often save information or create documents and save them to various types of computer-related storage devices, both internally, such as the hard drive, and externally, such as a thumb drive.
13. Your Affiant knows that computers are expensive and that people keep them in their possession for several years. Even after people buy a new computer they often do not dispose of their old computer. It is common for people to possess old computers for several years either because they do not want to dispose of an item that was expensive or because they do not know how to delete the personal information they have accrued on their computer.
14. Your Affiant knows from his training and experience, and the training and experience of other law enforcement personnel to whom your Affiant has spoken with, that those persons who possess, trade, receive or distribute images of minors engaged in sexually explicit conduct view children as sexual objects, and that such persons receive gratification from sexually explicit images of minors.
15. Your Affiant further knows that those who derive gratification from sexually explicit images of minors often engage in the exploitation and molestation of minors.
16. Your Affiant knows through his training and experience that during the engagement of sexual exploitation, those deriving gratification from a sexually explicit act may use items or objects to further the sexually explicit act. Due to the nature of the act,

fingerprints, trace evidence, and deoxyribonucleic acid (DNA) evidence may exist on the item or object.

17. Your Affiant knows from training and experience that those persons who possess, trade, receive, or distribute sexually explicit images of minors often maintain their sexually explicit images of minors, and that such images can include all types of media such as still photographs, digital photographs, video clips, digital video clips, printouts, magazines, and videotapes. From training and the training and experience of other agents to whom your Affiant has spoken with, many individuals interested in child pornography have admitted being addicted to the images and find sexual gratification in said images. Your Affiant knows that currently the most prevalent media used is digital media, including digital photographs and digital video clips that are stored on the possessor's computer hard drive, computer diskettes, CD ROM's, and various external computer memory storage devices, such as flash drives, thumb drives, key drives, USB devices, iPods, iPads, tablets, PSP Players, gaming systems, removable/portable hard drives, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media, some of which can be extremely small and stored easily in personal safes, lockboxes, vehicles, or on one's person. Additionally, your Affiant knows from training and experience, that digital images are easily printable in "hard copy" form and can be stored virtually anywhere inside a residence, vehicle, boat, garage, sheds, bank safety deposit boxes, lock boxes, and personally owned safes, as well as other areas under the control of those persons possessing, distributing, and receiving sexually explicit images of minors.
18. Further, your Affiant knows that digital media storage devices including "thumb drives," "flash drives", "pen drives", or memory sticks are by their very nature designed to be small enough to carry in one's pocket or affixed to a key chain. Also, your Affiant is aware that digital cameras and video recording devices contain storage disks that are like "thumb drives," in that they can hold large quantities of data, and come in very small sizes. Your Affiant knows that such storage devices are able to store digital images, and by their nature are extremely portable and can easily be concealed on one's person or in one's clothing. The extremely portable and valuable nature of these digital images may also be stored in a person's vehicle
19. Your Affiant knows that many cellular telephones, "smart phones," and Personal Digital Assistants (PDA's) are capable of receiving, distributing and possessing child pornography images through infrared transmissions as a picture message or attachment to a text message sent to or received from other cellular telephones, PDA's, and computers. Many models of cellular telephones and PDA's have two storage capabilities. The device may have built-in memory capable of holding child pornography images and also utilize removable storage options capable of holding child pornography images (such as compact flash cards, secure digital cards, and memory sticks). Many of these storage cards are capable of being read by computers, other cellular telephones, PDA's, and can be loaded directly onto printers.

20. Your Affiant knows that cellular telephones, which utilize computer technology, serve basic functions in connection with child pornography, including production.
21. Your Affiant knows that a cellular telephone has the ability to take photographs or videos, and store those images and videos in digital form, making the cellular telephone itself an ideal repository for child pornography production. Additionally, cellular telephones are portable and capable of being stored on one's person.
22. Many models of cellular telephones have two data storage capabilities. The device may have built-in memory capable of holding images and videos, and also utilize one or more removable storage options such as compact flash cards, secure digital cards, memory sticks, and others. Many of these storage cards are capable of being read by computers, other cellular telephones, PDAs, other digital cameras and can be loaded directly into some printers.
23. Your affiant knows that a subscriber identity module or "sim card" is utilized in cellular telephone technology. The sim card can store data for telephone subscribers such as user identity information, location information, subscriber phone number, network authorization data, personal security keys, contact lists, and stored text messages.
24. As further described in Attachment B, this warrant seeks permission to search and seize certain records related to 18 U.S.C. 2252 and 2251 that exists in the items more fully described in Attachment A in whatever form they are found. One form in which the records may be found is stored on a computer's hard drive or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records may be in a form that becomes meaningful only upon forensic analysis.
25. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture and movie files), computer hard drives can contain other forms of electronic evidence that are not user-generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used and who has used these records. For instance, based upon your Affiant's knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, your Affiant knows:
 - a. Data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
 - b. Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes the computer were recently in use.

c. Web browsers, e-mail programs and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords.

d. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices and the times the computer was in use.

e. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information may be evidence of a crime or indicate the existence and location of evidence in other locations on the hard drive.

26. Further, in finding evidence of how a computer has been used, the purposes for which it was used and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based on your Affiants knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, your affiant knows that when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, and, for example, by reviewing the Index.dat files (a system file that keeps track of historical activity conducted in the Internet Explorer application), whether a user accessed other information close in time to the file creation dates, times and sequences so as to establish user identity and exclude others from computer usage during times related to the criminal activity.

27. Evidence of how a digital device has been used, what it has been used for and who has used it, may be the absence of particular data on a digital device and requires analysis of the digital device as a whole to demonstrate the absence of particular data. Evidence of the absence of particular data on a digital device is not segregable from the digital device.

28. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge and intent.

29. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to

understand the evidence described in Attachment B also falls within the scope of the warrant.

30. Based upon Your Affiants knowledge, training and experience, as well as information related your affiant by agents and others involved in the forensic examination of digital devices, your Affiant knows that it is necessary to seize all types of electronic devices capable of storing digital evidence as described in this Affidavit and Attachment B for off-site review because computer searches involve highly technical, complex and dynamic processes.
31. Your Affiant knows through training and experience that individuals that show an interest in visual depictions of minors engaged in sexually explicit conduct may have in their possession journals correspondence and other writings detailing their and others involvement with visual depictions of minors engaged in sexually explicit conduct or a sexual interest in children. Your Affiant knows that these individuals may also keep records related to their internet service provider and internet services.

Details of the Investigation

32. On July 24, 2015, the Federal Bureau of Investigation was contacted by Deputy David Zilink of the Valencia County Sheriff's Office regarding the possible production of child pornography.
33. Deputy Zilink stated that on July 14, 2015, he was assigned a case regarding the criminal sexual penetration of Jane Doe, who was eight years of age at the time of the alleged incident.
34. Deputy Zilink learned through conversations with Detective Sergeant Don Derrick of the Valencia County Sheriff's Office that the mother of the child victim, Ms. Chavez, and the child victim, Jane Doe, fled the state of New Mexico due safety concerns. Once in a safe place, Ms. Chavez contacted the local authorities in Spokane, Washington to make a complaint. Ms. Chavez said that the sexual acts that were being performed on Jane Doe were by her ex-boyfriend whom she identified as Martin Perea, hereinafter referred to as, PEREA.
35. According to the police report by Officer Jerod Beasley of Spokane Police Department, on July 3, 2015, Officer Beasley was dispatched to the Deaconess Hospital regarding a delayed report of rape occurring in New Mexico.
36. Ms. Chavez told Officer Beasley that she had dated PEREA for approximately seven years and had been separated for the last two months.
37. On July 1, 2015, while at PEREA's residence located at 52 Buena Vista Street, Los Lunas, New Mexico, Ms. Chavez decided to search PEREA's cellular telephone to find evidence of his infidelity. Ms. Chavez took the memory card out of PEREA's cellular telephone. While searching the memory card, Ms. Chavez discovered digital

photographs and videos dating back to September 2014 of someone “hurting her daughter.” When asked what she meant, Ms. Chavez explained that there were videos on the memory card of her daughter naked and someone forcibly spreading her legs and inserting a pen inside Jane Doe’s vagina. Ms. Chavez said there were several videos and pictures of someone inserting several items into Jane Doe’s vagina including a pen, marker, and a finger. Ms. Chavez stated she was able to identify Jane Doe by her pajamas in some videos and pictures and others Ms. Chavez could clearly identify Jane Doe’s face. Ms. Chavez believed that PEREA was the one performing the sexual acts.

38. The same day, Ms. Chavez confronted PEREA about the digital photographs and videos of Jane Doe found on the memory card taken from PEREA’s cellular telephone. PEREA stated that he was sorry that he had the images and videos on his memory card, and that he only did it because Ms. Chavez had not been intimate with him.
39. On July 2, 2015, Ms. Chavez met with PEREA. PEREA demanded that Ms. Chavez return the memory card to him or he would, “burn you [Ms. Chavez] and the house [Ms. Chavez’s residence at 1303 Ajay Place] down.”
40. Around midnight of July 3, 2015, Ms. Chavez fled New Mexico with all her children out of fear of her safety, the safety of Jane Doe, and the safety of her twin seven year old sons.
41. Ms. Chavez handed Officer Beasley the memory card that she took from PEREA. The memory card was placed into evidence at the Spokane Police Department.
42. Deputy Zilink contacted Detective Lamanna of the Spokane Police Department and had the memory card transferred to the care, custody, and control of the Valencia County Sheriff’s Office.
43. On July 28, 2015, agents with the FBI obtained a search warrant for the memory card at the United States District Court of New Mexico. The warrant was executed the same day at the New Mexico Regional Computer Forensics Laboratory. The execution involved the download of the contents of the memory card.
44. The memory card contained approximately 111 video files, and over 980 image files. Out of the over 1,000 files, multiple video and image files were found to contain suspected child pornography. The following suspected child pornography files are described below:
 - a. File “39_20150114_233030” – 11:07 video dated on 01/14/2015 starts with a close-up of a prepubescent vagina that appears to be wet. A black and white striped blanket is at the lower portion of the screen. At the :30 mark, the right pinky of an adult male hand begins to rub the clitoris and inside the labia majora of the prepubescent girl; the pinky and other finger

appear to be coated in lubricant. At the 1:00 mark, the right index finger of the adult male hand begins to rub the clitoris area of the prepubescent girl. At the 1:12 mark, the adult male hand spreads open the labia majora, and then digitally penetrates the prepubescent girl. As the adult male hand repeatedly penetrates the vagina with his index finger, a tattoo between the index finger and the thumb on the right hand is clearly visible. The tattoo is black in color and looks to be older. The tattoo appears to contain the letter "M." The adult male hand then switches penetration of the prepubescent vagina to his pinky finger. At approximately 1:46, it appears that the prepubescent girl is disturbed, indicated by a sudden flinch and moving away from the adult male hand. At 1:52 the tattoo is seen again and the camera rapidly moves around. A black and white striped blanket and a blue mattress are clearly visible in the video. The male hand again spreads open the labia majora, and strokes several different fingers inside the labia majora of the prepubescent girl. At the 3:00 mark, a purple marker can be seen inserted inside the vagina repeatedly. At 3:03, the prepubescent girl moves away, and the side of the marker clearly reads, "playful purple." At 3:28 the adult male asks, "Are you awake?" At approximately 5:06 in the video, the prepubescent girl closes her legs trapping the marker and the adult male hand between her thighs. At 5:43 an object wrapped in clear tape can be seen inserted repeatedly in the prepubescent girl's vagina. The object looks to have a black cap similar to a Sharpie marker. At 7:50, the male can be heard whispering, "Go to sleep." At 8:12, a blue Sea World pen with clear plastic tape wrapped around the marked end can be seen inserted repeatedly into the prepubescent girl's vagina. At 8:39 the right index finger of an adult male can be seen rubbing the clitoris of the prepubescent vagina. The adult male whispers excitedly, "That's good." At 9:35, a orange colored oil can be seen being poured onto a prepubescent girl's vagina. Based on training and experience the girl appears to be between the ages of 6 and 10 years of age.

- b. File "52_20150117_040552" – 7:26 video dated on 01/17/2015 showing the full body of Jane Doe asleep lying on her right side on top of a bed. Jane Doe is wearing a pink pajama top with a bear embroidered on the upper left chest area. Jane Doe is also wearing light pink pajama bottoms with a teddy bear print. The pajama bottoms are around her ankles and she is not wearing underwear. Jane Doe also is wearing pink socks. There is a yellow, blue, white, and pink blanket positioned behind her body, and the sheets appear to be black in color. The audio of a television can be heard in the background. The camera zooms into the genital area of Jane Doe, and a male hand comes into view to spread the labia majora of the vagina. The male hand appears to put lubricant onto the vagina. Around the 2:10 mark an object wrapped in black electrical tape is inserted into the vagina. The object is moved repeatedly in and out of the vagina. At the 4:30 mark, a Bic "mark-it" blue marker that reads, "Fine point permanent marker"

and a handwritten, "Maria" is repeatedly inserted into the vagina. At the 6:31 mark, the black electrical tape wrapped object is inserted again into the vagina. Jane Doe appeared to be woken up and quickly moves. Jane Doe is 8 years old.

- c. File "48_20150115_001054" – :40 video dated on 01/14/2015 starts with an adult male's hand uncovering a black colored bed spread to reveal a naked prepubescent vagina. The legs of the prepubescent girl are spread by the adult male's hand. The prepubescent girl appears to be on top of a blue colored mattress, also visible is a pink, white and black blanket, as well as a black and white striped blanket. The labia majora appears to be wet. An orange colored bottle comes into view and at the: 16 mark, an orange colored oil is poured onto the prepubescent vagina. The right index finger of the male begins to rub the clitoris and inside the labia majora of the prepubescent girl. At the: 34 second mark, the video cuts to a side angle shot from the right side of the prepubescent girl. The left side of an adult male face is visible as the adult male performs oral sex on the prepubescent girl. Based on training and experience the girl appears to be between the ages of 6 and 10 years of age.
 - d. File "51_20150117_040544" – A still image depicting Jane Doe asleep lying on her right side. The image appears to have been taken at the same time as the file referenced in subparagraph "b" above. The image was taken on the same day, 01/17/2015. The metadata shows that the camera used to take the image was a Samsung SCH-I545, which is a Samsung Galaxy S4.
 - e. File "160_IMG_20141009_033452" – A still image depicting Jane Doe asleep on a mattress covered in Pittsburgh Steelers bed sheets. Jane Doe is only wearing a red Dion's short sleeved t-shirt. Her legs are apart exposing her vagina. The photo was taken with a Broadcom 2157 cellular telephone. Jane Doe was seven years of age at the time the image was taken.
45. After viewing the images and videos, your Affiant spoke to Ms. Chavez. Ms. Chavez informed your Affiant that the details of the room and bedding matched the same room and bedding that Jane Doe occupied.
46. Ms. Chavez also informed your Affiant that PEREA has an old, faded tattoo on his right hand between his thumb and index finger. The tattoo consists of PEREA's initials, "MP." Ms. Chavez only viewed a few of the videos and said that she did not notice that tattoo in the video because of the appalling nature. She did say that she knew it was PEREA because she said that after dating for approximately six years, she knew what PEREA's hands and fingers looked like.

47. On July 28, 2015, a forensic interview was conducted on Jane Doe. Jane Doe said that she knew the reason she was being interviewed, "Because of my fake dad, Martin." Jane Doe stated that PEREA rubbed "her privates" with his hand both over and underneath her underwear. Jane Doe stated that PEREA did this event multiple times and that no one else has ever done so before or after.
48. On August 4, 2015, PEREA was arrested by the FBI.
49. On August 25, 2015, the defendant was indicted with nine counts of 18 U.S.C. Sections 2251(a), (e), and 2256; specifically production of a visual depiction of a minor engaging in sexually explicit conduct.
50. On June 10, ^{2016 RE} ~~2015~~, your Affiant was contacted by Ms. Chavez. Ms. Chavez informed your Affiant that she was going through some of the items that had been removed from 1303 Ajay Place while she was in Washington. The items were removed by Ms. Chavez' sister sometime in early July 2015. The items were packed and transported by her sister and her sister's boyfriend in July 2015, and taken to her mother's shed located in Los Lunas, New Mexico. In early June 2016, Ms. Chavez retrieved the items from the shed.
51. Ms. Chavez discovered several 3.5 inch floppy disks, compact discs, as well as several cellular telephone sim cards. Ms. Chavez said that they belonged to PEREA. She knew the items belonged to PEREA because some of the floppy disks have PEREA's handwriting on the labels, and she did not possess a computer capable of reading 3.5 inch floppy disks, but that PEREA did. Several of the floppy disks have either "pics" or "pictures" written on their labels. Ms. Chavez stated that the sim cards, floppy disks, and compact discs seized were not hers. Ms. Chavez identified the items that belonged to her from the box in the presence of your Affiant.
52. Your Affiant confirmed that one of the computers seized from PEREA has the capability of reading 3.5 inch floppy disks.
53. On June 13, 2016 Your Affiant seized the items that are more fully described in Attachment B and took them back to the FBI Albuquerque Division office.

Interstate Nexus

54. Your Affiant believes that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. §§ 2251(a), 2252(a)(4)(B) and for the limited purpose of securing a search warrant.
55. The Government can demonstrate the images and videos were stored on an item manufactured outside New Mexico. Your Affiant is unaware, from his training and experience, of any computer hardware/digital media capable of holding data being manufactured in the state of New Mexico, other than the Intel processors produced at the Intel facility in Rio Rancho, New Mexico. Intel processors contain on-chip cache

memory that is volatile and not conducive for transporting stored data, not to be confused with hard drives, flash drives, or other non-volatile digital media that maintains the data after power is removed.

56. Further, the FujiFilm floppy disks were manufactured by FujiFilm USA in South Carolina, thus satisfying the interstate nexus element.

Computers and Computer Related Media in Child Pornography Investigations

57. Your Affiant knows based upon training, experience, and information relayed by law enforcement officers and others involved in the forensic examination of computers that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips as described in Attachment B. Searches and seizures of computers and computer-related media requires agents to seize all computers and computer-related media described in Attachment B to be processed by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:
- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.
 - b. Searching computer systems requires the use of precise scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.
 - c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.
 - d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily

change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

58. In order to search for data that is capable of being read or interpreted by a computer and computer-related media described in Attachment B, law enforcement personnel will need to search, seize, image, copy, and examine the following items believed to be evidence and/or an instrumentality of a violation of 18 U.S.C. 2252, subject to the procedures set forth above:

- a. All computer equipment and storage device which are capable of being used to commit or further the crimes outlined above, or create, access or store the types of evidence, fruits, or instrumentalities of such crimes as outlined in Attachment B;
- b. All computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners which are capable of being used to commit or further the crimes outlined above, or create, access or store the types of evidence, fruits, or instrumentalities of such crimes as outlined in Attachment B;
- c. All magnetic, electronic or optical storage devices capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic notebooks, cellular telephones, digital cameras, video cameras (both digital and analog), thumb drives, memory sticks, USB flash drives, key drives, USB devices, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), iPods, iPads, tablets, PSP players, gaming systems, printers, scanners, video game systems, Blu-ray discs, minidiscs, removable/portable hard drives, magnetic tapes, Video Home System tapes (VHS), ZIP drives and personal digital assistants capable of being used to commit or further the crimes outlined above, or create, access or store the types of evidence, fruits, or instrumentalities of such crimes as outlined in Attachment B;

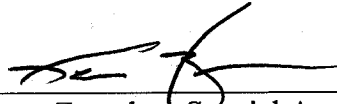
- d. All documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software.
- e. All applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;
- f. All internet service provider records;
- g. All physical keys, encryption devices, dongles, and similar physical items that are necessary to gain access to the computer equipment, storage devices or data;
- h. All passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
- i. Writing tablets, journals, correspondence and other written content evidence that may identify individual involvement.

Identification of the Property to be Examined

- 59. The property to be searched is described in Attachment A. The property is currently being stored at Federal Bureau of Investigation Office located at 4200 Luecking Park Avenue, Albuquerque, New Mexico 87107.
- 60. The applied-for search warrant would authorize the examination of the property for the purpose of identifying electronically stored data particularly described in Attachment B.

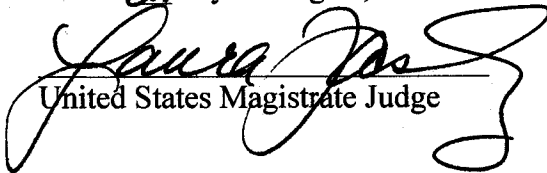
Conclusion

- 61. Based on the information set forth above, there is probable cause to believe that the computer related media described in Attachment B, located at the FBI Albuquerque Division office described in Attachment A, are instrumentalities and evidence of the sexual exploitation of minors, in violation Title 18 U.S.C. §§ 2251(a) and 2252(a)(4)(B). Furthermore, based upon the foregoing paragraphs, judicial authority is specifically requested to search computer storage devices, and other evidence outlined in Attachment B, and complete the search/examination of the computer related media at an appropriate law enforcement facility.
- 62. Assistant United States Attorney Shammara Henderson has reviewed and approved this affidavit for the application for a search warrant of the items more specifically described in Attachment B
- 63. I swear that this information is true and correct to the best of my knowledge.



Ross Zuercher, Special Agent - FBI

SUBSCRIBED and SWORN to before
me this 21st day of August, 2016.


United States Magistrate Judge

ATTACHMENT A

The property to be searched is described below:

- 1 - 3.5" Floppy FujiFilm – Tan color – w/label: "Hard drive 7510801.exe
6/22/03 – GWSCAN 3.15 – Release date 1/11/02"
 - 1 - 3.5" Floppy Verbatim – Tan color – w/label: "PEREA"
 - 5 - 3.5" Floppy Sony – Tan color – w/multi color labels, all blank
 - 1 - 3.5" Floppy Sony – Cream color – w/label: "Payments"
 - 4 - 3.5" Floppy Sony – Cream color – no labels
 - 1 - 3.5" Floppy IBM – Blue color – w/label: "Piercing Records"
 - 1 - 3.5" Floppy Sony – Blue color – w/label: "Doys(unreadable) Poems"
 - 1 - 3.5" Floppy Sony – Blue color – w/label: "Word files"
 - 4 - 3.5" Floppy Sony – Blue color – no labels
 - 1 - 3.5" Floppy IBM – Green color – w/label: "Wooble Pics"
 - 5 - 3.5" Floppy Sony – Green color – no labels
 - 1 - 3.5" Floppy Sony – Yellow color – w/label: "Bot II Files from Excel
Business Technician Mr. Perea"
 - 1 - 3.5" Floppy Sony – Yellow color – w/label: "Bot II Mr. Perea"
 - 1 - 3.5" Floppy Sony – Yellow color – w/label: "Pics Laura & Family"
 - 4 - 3.5" Floppy Sony – Yellow color – no labels
 - 1 - 3.5" Floppy Sony – Red color – w/label: "Word Files"
 - 1 - 3.5" Floppy Sony – Red color – w/label: "Y&Z Company/ inventory /order
sheets/ special orders"
 - 1 - 3.5" Floppy Sony – Red color – w/label: "Piercing Care Sheets"
 - 1 - 3.5" Floppy Sony – Red color – w/label: "Word Files"
 - 1 - 3.5" Floppy Sony – Red color – w/label: "My pics"
 - 1 - 3.5" Floppy Sony – Red color – w/label: "business Cards/ Wildland files"
 - 4 - 3.5" Floppy Sony – Red color – no labels
 - 1 - 3.5" Floppy Office Depot – Black color – w/label "Pictures Laura & family"
 - 1 - 3.5" Floppy Office Depot – Black color – w/label: "Pics"
 - 1 - 3.5" Floppy Office Depot – Black color – w/labels: "Reciepts"
 - 1 - 3.5" Floppy IBM – Bright Yellow – w/label: "Tina Pics"
 - 1 - 3.5" Floppy FujiFilm – Blue/Green Color: w/label: "Best of WEB Gold
Partz"
 - 1 - 3.5" Floppy Memorex – Clear Yellow – no label
-
- 1 – Verizon sim card with etched numbers: 89148000001485207772
 - 1 – T-Mobile sim cardwith etched numbers: 8901260573521731234
 - 1 – Memorex compact disc (red)
 - 1 – Memorex compact disc (blue)
 - 1 – TDK compact disc (silver)
 - 1 Maxwell digital video disc (gold)

ATTACHMENT B

All records on the property described in Attachment A that relate to violation of 18 U.S.C. Sections 2252(a)(4)(B) and 2251; specifically possession and production of child pornography, including:

1. All photographs (including negatives, still photos, video tapes, artists drawings, slides and any type of computer formatted photograph) which depict a minor posed or candid in a sexual manner.
2. All non-sexual photographs of minors who appear to be the same minors delineated in paragraph 3 above. Any information [including names, addresses, nick names, schools, after school groups] that may lead to the identity and age of any minor children depicted in any visual media seized pursuant to this search warrant.
3. All copies and originals of envelopes, letters, diaries, ledgers, journals, and other correspondence pertaining to the possession, receipt, distribution, production, and/or reproduction of visual depictions of a person under the age of 18 years engaging in or simulating sexual conduct.
4. All documentation, (whether on paper or stored magnetic, digital, or optical media) describing discussions by individuals within the property with any individual or entity concerning: the identity of persons that are sexually attracted toward children, members of child sex advocacy groups, child victims and other persons involved in the sexual exploitation of children.